DIGITAL DATA RECORDING AND REPRODUCTION SYSTEM

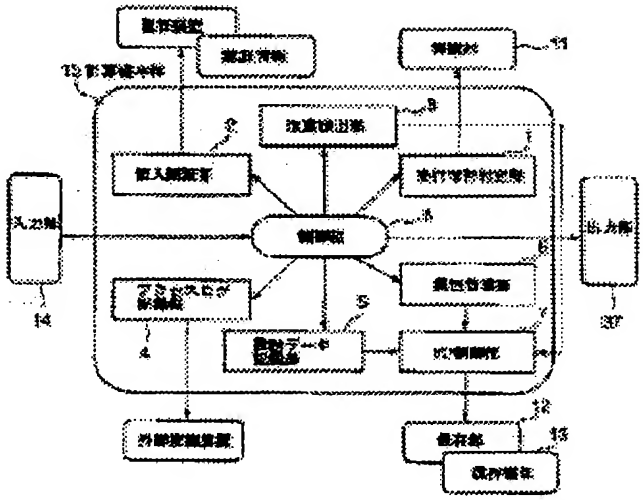
Publication number: JP2001036523
Publication date: 2001-02-09
Inventor: KOMATA YOSHINOBU; KONDO TAKASHI
Applicant: OLYMPUS OPTICAL CO
Classification:
- international: ***G09C1/00; G06F21/00; G11B20/10; H04L9/32; H04N7/167;*** **G09C1/00; G06F21/00; G11B20/10; H04L9/32; H04N7/167;** (IPC1-7): H04L9/32; G09C1/00; G11B20/10; H04N7/167
- European: G06F21/00N1T; G06F21/00N3J5; G06F21/00N3P; G06F21/00N3P2; G06F21/00N5A2B; G06F21/00N5A2D; G06F21/00N9A2
Application number: JP19990207982 19990722
Priority number(s): JP19990207982 19990722

Also published as:
US6477530 (B1)

Report a data error here

Abstract of **JP2001036523**

PROBLEM TO BE SOLVED: To obtain a system as a low cost data storage device that can be easily operated even when no network facility is available, by providing an execution propriety judging part to whether environment under which an operation control instruction is executed for each part is appropriate or not when operation control of each part is performed at a control part. SOLUTION: Data inputted in a data input part 14 is handled so as to perform a specified processing including storage in a data storage part 12 as digital data in a computer main body 15 based on the operation control instruction by the control part 8 to each part provided with the data storage part 12 and the computer main body 15. When the digital data is outputted from a data output part 37 by responding to the request, the environment under which the operation control instruction by the control part 8 for each part is executed is appropriate or not by cooperation with a protecting part 11 connected with the computer main body 15 by the execution propriety judging part 1. A digital data recording and reproduction system is provided with the protecting part 11 to be connected with the computer main body 15.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－36523
（P2001－36523A）
(43)公開日　平成13年２月９日(2001.2.9)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ	５Ｃ０６４
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｊ１０４
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ	９Ａ００１

審査請求　未請求　請求項の数14　ＯＬ　（全 23 頁）

(21)出願番号　特願平11－207982

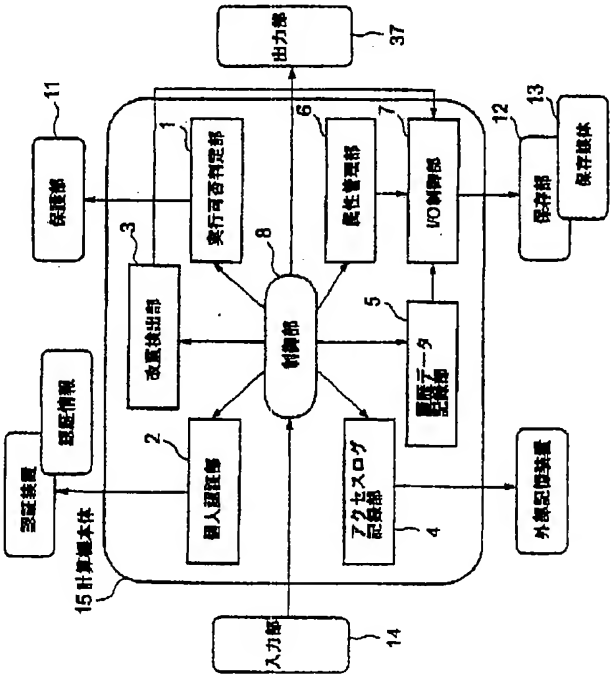
(22)出願日　平成11年７月22日(1999.7.22)

(71)出願人　000000376
オリンパス光学工業株式会社
東京都渋谷区幡ヶ谷２丁目43番２号
(72)発明者　小俣　芳信
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内
(72)発明者　近藤　隆
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外４名）

最終頁に続く

(54)【発明の名称】　デジタルデータ記録再生システム

(57)【要約】
【課題】本発明は、ネットワーク設備のない所でも容易に運用することができる低コストのデータ保存装置として実現することが可能なデジタルデータ記録再生システムを提供する。
【解決手段】本発明によると、データ入力部と、計算機本体と、データ出力部とからなり、前記データ入力部により入力されたデータを前記計算機本体内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体は、データ保存部と、個人認証部、アクセスログ記録部、改竄検出部、履歴データ記録部、属性管理部のうちの少なくとも一つと、前記データ保存部及び前記個人認証部、アクセスログ記録部、改竄検出部、履歴データ記録部、属性管理部のうち前記計算機本体が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部と、前記制御部による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部とを備えることを特徴とする。



【特許請求の範囲】
【請求項１】　データ入力部と、計算機本体と、データ出力部とからなり、前記データ入力部により入力されたデータを前記計算機本体内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、
前記計算機本体は、
デジタルデータを記憶するデータ保存部と、
当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部と、前記利用者が前記データ保存部に対してアクセスしたことを記録するアクセスログ記録部と、前記データ保存部に記憶されたデータが改竄されたか否かを検出する改竄検出部と、前記データ保存部に記憶されたデータに関する変更・修正情報を記録する履歴データ記録部と、前記データ保存部に記憶されたデータの属性を管理する属性管理部とのうちの少なくとも一つと、
前記データ保存部及び前記個人認証部、アクセスログ記録部、改鼠検出部、履歴データ記録部、属性管理部のうち前記計算機本体が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部と、
前記制御部による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部と、
を備えることを特徴とするデジタルデータ記録再生システム。
【請求項２】　前記デジタルデータ記録再生システムは、
さらに、前記計算機本体に接続された保護部を備え、
前記保護部は、前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を格納する読み出し専用不揮発性メモリとを備え、
前記実行可否判定部は、前記保護部との通信により、前記読み出し専用不揮発性メモリに格納されている前記ホスト識別子を取得することにより、前記動作制御命令を実行する環境が正当な環境であるか否かを判定することを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項３】　前記実行可否判定部は、
前記計算機本体に備えられた中央演算装置にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行なうことを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項４】　前記実行可否判定部は、
複数の独立したホスト識別子読み取り部を備えたことを特徴とする請求項２記載のデジタルデータ記録再生システム。
【請求項５】　前記複数の独立したホスト識別子読み取り部は、相互に確認を行うことにより、互いが正当なホスト識別子読み取り部であることを確認することを特徴とする請求項４記載のデジタルデータ記録再生システム。
【請求項６】　前記個人認証部は、
認証情報が書き込まれたＩＣカードと、
前記ＩＣカードに書き込まれた認証情報を読み取るＩＣカード読取部とを備え、
前記個人認証部とＩＣカード読取部との間の通信に暗号化通信を用いることを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項７】　前記個人認証部は、
生体情報を入力するための生体情報入力部を備え、
前記生体情報入力部により入力された生体情報に基づいて個人認証を行うことを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項８】　前記改竄検出部は、
前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、
前記保存部の各データファイルから所定の算出式に基づいて計算される照合用電子署名と、
を照合する照合部とを備えることを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項９】　前記改竄検出部は、
前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、
前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用電子署名と、
を照合するための照合部とを備えることを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項１０】　前記アクセスログ記録部は、利用開始あるいは利用終了日時と、利用者を識別するための利用者名と、利用開始あるいは利用終了の種別と、を前記データ保存部に記録することを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項１１】　前記履歴データ記録部は、
履歴データとして利用者を識別するための使用者名と、利用の日時を示す利用日時と、利用者がどのような作業を行ったかを示すアクセス種別と、使用した保存装置を特定するための保存装置識別子と、を前記データ保存部へ記録することを特徴とする請求項１記載のデジタルデータ記録再生システム。
【請求項１２】　前記制御部は、
さらに、前記データ保存部内の保存媒体上のデータにアクセスするためのＩ／Ｏ制御部を備え、
このＩ／Ｏ制御部は、
前記保存媒体を識別するための保存媒体識別部と、
データの情報を暗号化するための暗号化部と、
暗号化されたデータを復号するための復号化部とを備えることを特徴とする請求項１記載のデジタルデータ記録再生システム。

【請求項１３】　前記暗号化部と復号化部は、
それぞれ階層的な構造により暗号化レベルを変化することができることを特徴とする請求項１２記載のデジタルデータ記録再生システム。
【請求項１４】　前記属性管理部は、
少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、
データがバックアップであることを示すバックアップ識別子とを管理することを特徴とする請求項１記載のデジタルデータ記録再生システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタルデータを保存するためのデジタルデータ記録再生システムに関し、例えば、光磁気ディスクなどの着脱可能でかつ書き換え可能な記録媒体にデジタルデータを保存するデジタルデータ記録再生システムに関する。
【０００２】
【従来の技術】近年、パーソナルコンピュータなどの計算機の普及に伴い、各種の情報がデジタルデータとして記録媒体に保存されるようになってきている。
【０００３】しかるに、計算機上で取り扱われるデジタルデータは、一般に、そのデータの複製、データの改竄などを容易に行うことができるので、データの保護やデータのセキュリティという観点からみると大きな問題となっている。
【０００４】このような問題を解決するため、近時、公表されている「原本性保証電子保存システムの開発」（創造的ソフトウエア育成事業及びエレクトリック・コマース推進事業に係る最終成果発表会１９８８）においては、２台の計算機をそれぞれ保存装置とホスト装置というように位置づけ、それらをＬＡＮなどのネットワークで接続して使用している。
【０００５】ここで、保存装置とは、実際にデータが保存されている装置で、ネットワークコンピューティングの用語を使えば、サーバーということができる。
【０００６】また、ホスト装置とは、ユーザが利用する端末の役割を果たし、ネットワークコンピューティングの用語を使えば、クライアントに相当する。
【０００７】つまり、クライアント／サーバシステムをネットワーク上に構築することにより、データのアクセス方法に制約を加えることにより、データの機密性を高めるようにしている。
【０００８】
【発明が解決しようとする課題】しかしながら、このようなデータ保存装置とホスト装置とによるクライアント／サーバシステムをネットワーク上に構築することは、少なくとも２台以上の計算機を必要とし、非常に高価なシステムになり導入時のコストが非常に高くなる点で問題となっている。
【０００９】さらに、このようなデータ保存装置とホスト装置とによるクライアント／サーバシステムは、ネットワーク設備のない所では、運用することができないか、あるいは、ネットワーク設備からの導入が必要となるため、そのコストはさらに高くなるという問題がある。
【００１０】本発明は、上記の事情に鑑みてなされたもので、ネットワーク設備のない所でも容易に運用することができる低コストのデータ保存装置として実現することが可能なデジタルデータ記録再生システムを提供することを目的とする。
【００１１】
【課題を解決するための手段】本発明によると、上記課題を解決するために、（１）　データ入力部と、計算機本体と、データ出力部とからなり、前記データ入力部により入力されたデータを前記計算機本体内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体は、デジタルデータを記憶するデータ保存部と、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部と、前記利用者が前記データ保存部に対してアクセスしたことを記録するアクセスログ記録部と、前記データ保存部に記憶されたデータが改竄されたか否かを検出する改竄検出部と、前記データ保存部に記憶されたデータに関する変更・修正情報を記録する履歴データ記録部と、前記データ保存部に記憶されたデータの属性を管理する属性管理部とのうちの少なくとも一つと、前記データ保存部及び前記個人認証部、アクセスログ記録部、改鼠検出部、履歴データ記録部、属性管理部のうち前記計算機本体が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部と、前記制御部による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部と、を備えることを特徴とするデジタルデータ記録再生システムが提供される。
【００１２】また、本発明によると、上記課題を解決するために、（２）　前記デジタルデータ記録再生システムは、さらに、前記計算機本体に接続された保護部を備え、前記保護部は、前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を格納する読み出し専用不揮発性メモリとを備え、前記実行可否判定部は、前記保護部との通信により、前記読み出し専用不揮発性メモリに格納されている前記ホスト識別子を取得することにより、前記動作制御命令を実行する環境が正当な環境であるか否かを判定することを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。
【００１３】また、本発明によると、上記課題を解決するために、（３）　前記実行可否判定部は、前記計算機本体に備えられた中央演算装置にあらかじめ書き込まれ

ている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行なうことを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００１４】また、本発明によると、上記課題を解決するために、（４）　前記実行可否判定部は、複数の独立したホスト識別子読み取り部を備えたことを特徴とする（２）記載のデジタルデータ記録再生システムが提供される。

【００１５】また、本発明によると、上記課題を解決するために、（５）　前記複数の独立したホスト識別子読み取り部は、相互に確認を行うことにより、互いが正当なホスト識別子読み取り部であることを確認することを特徴とする（４）記載のデジタルデータ記録再生システムが提供される。

【００１６】また、本発明によると、上記課題を解決するために、（６）　前記個人認証部は、認証情報が書き込まれたＩＣカードと、前記ＩＣカードに書き込まれた認証情報を読み取るＩＣカード読取部とを備え、　前記個人認証部とＩＣカード読取部との間の通信に暗号化通信を用いることを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００１７】また、本発明によると、上記課題を解決するために、（７）　前記個人認証部は、生体情報を入力するための生体情報入力部を備え、前記生体情報入力部により入力された生体情報に基づいて個人認証を行うことを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００１８】また、本発明によると、上記課題を解決するために、（８）　前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、前記保存部の各データファイルから所定の算出式に基づいて計算される照合用電子署名と、を照合する照合部とを備えることを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００１９】また、本発明によると、上記課題を解決するために、（９）　前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名と、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用電子署名と、を照合するための照合部とを備えることを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００２０】また、本発明によると、上記課題を解決するために、（１０）　前記アクセスログ記録部は、利用開始あるいは利用終了日時と、利用者を識別するための利用者名と、利用開始あるいは利用終了の種別と、を前記データ保存部に記録することを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００２１】また、本発明によると、上記課題を解決するために、（１１）　前記履歴データ記録部は、履歴データとして利用者を識別するための使用者名と、利用の日時を示す利用日時と、利用者がどのような作業を行ったかを示すアクセス種別と、使用した保存装置を特定するための保存装置識別子と、を前記データ保存部へ記録することを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００２２】また、本発明によると、上記課題を解決するために、（１２）　前記制御部は、さらに、前記データ保存部内の保存媒体上のデータにアクセスするためのＩ／Ｏ制御部を備え、このＩ／Ｏ制御部は、前記保存媒体を識別するための保存媒体識別部と、データの情報を暗号化するための暗号化部と、暗号化されたデータを復号するための復号化部とを備えることを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００２３】また、本発明によると、上記課題を解決するために、（１３）　前記暗号化部と復号化部は、それぞれ階層的な構造により暗号化レベルを変化することができることを特徴とする（１２）記載のデジタルデータ記録再生システムが提供される。

【００２４】また、本発明によると、上記課題を解決するために、（１４）　前記属性管理部は、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを管理することを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。

【００２５】

【発明の実施の形態】以下図面を参照して本発明の実施の形態について説明する。

【００２６】図１は、本発明の一実施の形態として適用されるデジタルデータ記録再生システムの構成を示すブロック図である。

【００２７】すなわち、図１に示すように、このデジタルデータ記録再生システムは、キーボード等の入力手段を含むデータ入力部１４と、パーナルコンピュータ（ＰＣ）等の計算機本体１５と、ディスプレィ等の表示手段を含むデータ出力部３７とからなり、前記データ入力部１４により入力されたデータを前記計算機本体１５内でデジタルデータとして取り扱うと共に、それを前記データ出力部３７から出力するように構成されている。

【００２８】このデジタルデータ記録再生システムにおいて、前記計算機本体１５には、Ｉ／Ｏ制御部７を介してデジタルデータを記憶するデータ保存部１２が接続されている。

【００２９】そして、前記計算機本体１５内には、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部２と、前記利用

者が前記データ保存部１２に対してアクセスしたことを記録するアクセスログ記録部４と、前記データ保存部１２に記憶されたデータが改竄されたか否かをＩ／Ｏ制御部７を介して検出する改竄検出部３と、前記データ保存部１２に記憶されたデータに関する変更・修正情報をＩ／Ｏ制御部７を介して記録する履歴データ記録部５と、前記データ保存部１２に記憶されたデータの属性をＩ／Ｏ制御部７を介して管理する属性管理部６とが備えられている。

【００３０】また、この計算機本体１５内には、前記データ保存部１２及び前記個人認証部２、アクセスログ記録部４、改竄検出部３、履歴データ記録部５、属性管理部６の各々に対して動作命令を与えることにより、各部の動作制御を行う制御部８と、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境か否かを判定する実行可否判定部１とが備えられている。

【００３１】また、デジタルデータ記録再生システムは、さらに、前記計算機本体１５に接続された保護部１１を備えている。

【００３２】なお、図１では、デジタルデータを記憶するデータ保存部１２は、Ｉ／Ｏ制御部７を介して計算機本体１５に接続されている場合について説明したが、計算機本体１５内に備えられていてもよい。

【００３３】そして、このようなデジタルデータ記録再生システムでは、前記データ保存部１２及び前記計算機本体１５が備えている各部に対する前記制御部８による動作制御命令に基づいて、前記データ入力部１４により入力されたデータを前記計算機本体１５内でデジタルデータとしてデータ保存部１２への保存を含む所定の処理を施すように取り扱うと共に、それを要求に応じて前記データ出力部３７から出力する際に、前記実行可否判定部１が、前記計算機本体１５に接続された保護部１１との協働により、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境か否かを判定するようにしている。

【００３４】ここで、実行可否判定部１は、前記計算機本体１５に接続された保護部１１との協働により、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境であると判定したときには前記計算機本体１５による各部の処理を続行し、正当な環境でないと判定したときには前記計算機本体１５による各部の処理が中止される。

【００３５】ただし、実行可否判定部１は、前記計算機本体１５で内部的に、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境か否かを判定することができる場合には、前記計算機本体１５に接続された保護部１１との協働を要しない。

【００３６】なお、前記計算機本体１５が備えている各部とは、前記個人認証部２、アクセスログ記録部４、改竄検出部３、履歴データ記録部５、属性管理部６のうちの少なくとも一つを含むものとする。

【００３７】従って、このようなデジタルデータ記録再生システムでは、従来の原本性保証電子保存システムのようにクライアント／サーバシステムをネットワーク上に構築することによってデータのアクセス方法に制約を加えることにより、データの機密性を高めるようにすることなく、簡易でしかも低コストで原本性保証電子保存システムとほぼ等価な機能が得られるようになるものである。

【００３８】すなわち、以上のような図１の実施形態によると、データ入力部１４と、計算機本体１５と、データ出力部３７とからなり、前記データ入力部１４により入力されたデータを前記計算機本体１５内でデジタルデータとして取り扱うデジタルデータ記録再生システムにおいて、前記計算機本体１５は、デジタルデータを記憶するデータ保存部１２と、当該デジタルデータ記録再生システムを利用する利用者が正当な利用者か否かを確認する個人認証部２と、前記利用者が前記データ保存部１２に対してアクセスしたことを記録するアクセスログ記録部４と、前記データ保存部１２に記憶されたデータが改竄されたか否かを検出する改竄検出部３と、前記データ保存部１２に記憶されたデータに関する変更・修正情報を記録する履歴データ記録部５と、前記データ保存部１２に記憶されたデータの属性を管理する属性管理部６のうちの少なくとも一つと、前記データ保存部１２及び個人認証部２、アクセスログ記録部４、改竄検出部３、履歴データ記録部５、属性管理部６のうち前記計算機本体１５が備えている構成各々に対して動作命令を与えることにより、各部の動作制御を行う制御部８と、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判定する実行可否判定部１とを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【００３９】（実行可否判定部１による実行可否判定の具体例）次に、以上のような図１の実施形態における実行可否判定部１による実行可否判定の具体例について説明する。

【００４０】（第１の具体例）図２は、実行可否判定部１による実行可否判定の第１の具体例を示す要部の構成図である。

【００４１】図２に示すように、実行可否判定部１は、前記計算機本体１５に接続された保護部１１の読み出し専用不揮発性メモリ（ＥＥＰＲＯＭ等）１１ａにあらかじめ格納されている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子１６を取得することにより、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判断する。

【００４２】この場合、ホスト識別子１６は、一意のデータである。

【００４３】はじめに、実行可否判定部１は、前記計算機本体１５のＩ／Ｏポートに接続されている保護部１１に対してホスト識別子取得要求を送信する。

【００４４】これに応じて、保護部１１では、実行可否判定部１からのホスト識別子取得要求が正当なものと判断されたときには、実行可否判定部１に対して読み出し専用不揮発性メモリ１１ａにあらかじめ格納されているホスト識別子１６を読み出して送信する。

【００４５】このとき、実行可否判定部１と保護部１１とにおける両者間のデータの送受信は、専用の通信手段にて行われるものとする。

【００４６】実行可否判定部１では、受信したホスト識別子１６が正しい識別子であるか否かを判断し、このホスト識別子１６が正しいと判定したときには前記計算機本体１５による各部のときには処理を続行し、このホスト識別子１６が正しくないと判定したときには前記計算機本体１５による各部の処理が中止される。

【００４７】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムは、さらに、前記計算機本体１５に接続された保護部１１を備え、前記保護部１１は、前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子１６を格納する読み出し専用不揮発性メモリ１１ａとを備え、前記実行可否判定部１は、前記保護部１１との通信により、前記読み出し専用不揮発性メモリ１１ａに格納されている前記ホスト識別子を取得することにより、前記動作制御命令を実行する環境が正当な環境であるか否かを判定することを特徴とするデジタルデータ記録再生システムが提供される。

【００４８】（第２の具体例）図３は、実行可否判定部１による実行可否判定の第２の具体例を示す要部の構成図である。

【００４９】図３に示すように、実行可否判定部１は、前記計算機本体１５に備えられている中央演算装置１７にあらかじめ格納されているホスト識別子１６を取得することにより、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判断する。

【００５０】この場合、ホスト識別子１６は、例えば、製造時などに書き込まれる一意のデータである。

【００５１】はじめに、実行可否判定部１は、前記計算機本体１５に備えられている中央演算装置１７に対してホスト識別子取得要求を送信する。

【００５２】そして、中央演算装置１７では、実行可否判定部１からのホスト識別子取得要求を受信すると、実行可否判定部１に対してホスト識別子１６を送信する。

【００５３】実行可否判定部１では、受信したホスト識別子１６が正しい識別子であるか否かを判断し、このホスト識別子１６が正しいと判定したときには前記計算機本体１５による各部のときには処理を続行し、このホスト識別子１６が正しくないと判定したときには前記計算機本体１５による各部の処理が中止される。

【００５４】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記実行可否判定部は、前記計算機本体１１に備えられた中央演算装置１７にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子１６を読み出して判定を行なうことを特徴とするデジタルデータ記録再生システムが提供される。

【００５５】（第３の具体例）図４は、実行可否判定部１による実行可否判定の第３の具体例を示す要部の構成図である。

【００５６】図４に示すように、ｎ個のホスト識別子読み取り部ａ～ｎ（１８～２０）を備えている実行可否判定部１は、前記計算機本体１５に接続された保護部１１の読み出し専用不揮発性メモリ１１ｂにあらかじめ格納されている前記動作制御命令が実行される環境が正当な環境であることを保証するためのデータ列ａ～ｎ（２１～２３）からなるホスト識別子１６を取得することにより、前記動作制御命令を実行する環境が正当であるか否かを判断する。

【００５７】この場合、データ列ａ～ｎ（２１～２３）からなるホスト識別子１６は、それぞれ、一意のデータである。

【００５８】ここで、データ列ａ～ｎは、ホスト識別子１６をｎ個に分割したもので、データ列ａからデータ列ｂというようにデータ列ｎまでが順次結合されたとき、１つのホスト識別子を表すことができる。

【００５９】はじめに、実行可否判定部１は、ｎ個のホスト識別子読み取り部ａ～ｎ（１８～２０）までを同時に起動する。

【００６０】起動されたホスト識別子読み取り部１８～２０は、前記計算機本体１５のＩ／Ｏポートに接続されている保護部１１に対してホスト識別子１６のデータ列２１～２３の取得要求を送信する。

【００６１】このとき、実行可否判定部１では、各ホスト識別読み取り部１８～２０に対して、あらかじめ、保護部１１側のホスト識別子１６のうちどのデータ列２１～２３を読み込むか指示しておくものとする。

【００６２】保護部１１では、ホスト識別読み取り部１８～２０が、どのデータ列２１～２３の取得要求をしているのかに応じて、ホスト識別読み取り部１８～２０に対応するデータ列２１～２３を読み出し専用不揮発性メモリ１１ｂから読み出して送信する。

【００６３】このとき、実行可否判定部１と保護部１１とにおける両者間のデータの送受信は、専用の通信手段にて行われるものとする。

【００６４】ホスト識別子読み取り部１８～２０は、受信したデータ列２１～２３を直ちに実行可否判定手段１

に送信する。

【００６５】実行可否判定手段１では、データ列２１～２３の再構成を行い、受信したホスト識別子１６が正しい識別子であるか否かを判断し、このホスト識別子１６が正しいと判定したときには前記計算機本体１５による各部のときには処理を続行し、このホスト識別子１６が正しくないと判定したときには前記計算機本体１５による各部の処理が中止される。

【００６６】このように、第３の具体例では、同時アクセスとデータ列の順番を入れ替えることにより、耐リバースエンジニアリング性能が高くなる。

【００６７】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記実行可否判定部は、複数の独立したホスト識別子読み取り部を備えたことを特徴とするデジタルデータ記録再生システムが提供される。

【００６８】（第４の具体例）図５は、実行可否判定部１による実行可否判定の第４の具体例を示す要部の構成図である。

【００６９】図５に示すように、ｎ個のホスト識別子読み取り部ａ～ｎ（１８～２０）を備えている実行可否判定部１は、前記計算機本体１５に接続された保護部１１の読み出し専用不揮発性メモリ１１ｂにあらかじめ格納されているデータ列ａ～ｎ（２１～２３）からなるホスト識別子１６を取得することにより、前記動作制御命令を実行する環境が正当であるか否かを判断する。

【００７０】この場合、ホスト識別子１６は、前記動作制御命令を実行する環境が正当であることを保証するための、一意のデータである。

【００７１】ここで、データ列ａ～ｎは、ホスト識別子１６をｎ個に分割したもので、データ列ａからデータ列ｂというようにデータ列ｎまでが順次結合されたとき、１つのホスト識別子を表すことができる。

【００７２】はじめに、実行可否判定部１は、ｎ個のホスト識別子読み取り部ａ～ｎ（１８～２０）までを同時に起動する。

【００７３】起動されたｎ個のホスト識別子読み取り部１８～２０は、各ホスト識別子読み取り部が正当なものであるか否かを確認するため、各ホスト識別子読み取り部１８～２０の間で通信を行う。

【００７４】例えば、ホスト識別子読み取り部ａ（１８）がホスト識別子読み取り部ｂ（１９）を確認するために、ホスト識別子読み取り部ａ（１８）がホスト識別子読み取り部ｂ（１９）に識別コードＡ（２４）を送信し、ホスト識別子読み取り部ｂ（１９）ｂでは、識別コードＡ（２４）を受信してそれに対応する識別コードＢ（２５）をホスト識別子読み取り部ｃに送るというように、最終的にホスト識別子読み取り部ａ（１８）に適切なコードを受信することで各ホスト識別子読み取り部１８～２０の正当性を確認しあう。

【００７５】すべての各ホスト識別子読み取り部１８～２０の正当性が確認されると、各ホスト識別子読み取り部１８～２０は、前記計算機本体１５のＩ／Ｏポートに接続されている保護部１１に対してホスト識別子１６のデータ列２１～２３の取得要求を送信する。

【００７６】このとき、実行可否判定部１では、各ホスト識別読み取り部１８～２０に対して、あらかじめ、保護部１１側のホスト識別子１６のうちどのデータ列２１～２３を読み込むか指示しておくものとする。

【００７７】保護部１１では、ホスト識別読み取り部１８～２０が、どのデータ列２１～２３の取得要求をしているのかに応じて、ホスト識別読み取り部１８～２０に対応するデータ列２１～２３を読み出し専用不揮発性メモリ１１ｂから読み出して送信する。

【００７８】このとき、実行可否判定部１と保護部１１とにおける両者間のデータの送受信は、専用の通信手段にて行われるものとする。

【００７９】ホスト識別子読み取り部１８～２０は、受信したデータ列２１～２３を直ちに実行可否判定手段１に送信する。

【００８０】実行可否判定手段１では、データ列２１～２３の再構成を行い、受信したホスト識別子１６が正しい識別子であるか否かを判断し、このホスト識別子１６が正しいと判定したときには前記計算機本体１５による各部のときには処理を続行し、このホスト識別子１６が正しくないと判定したときには前記計算機本体１５による各部の処理が中止される。

【００８１】このように、第４の具体例では、同時アクセスとデータ列の順番を入れ替えることにより、耐リバースエンジニアリング性能が高くなる。

【００８２】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記複数の独立したホスト識別子読み取り部は、相互に確認を行うことにより、互いが正当なホスト識別子読み取り部であることを確認することを特徴とするデジタルデータ記録再生システムが提供される。

【００８３】（個人認証部２による個人認証の具体例）次に、以上のような図１の実施形態における個人認証部２による個人認証の具体例について説明する。

【００８４】（第１の具体例）図６は、個人認証部２による個人認証の第１の具体例を示す要部の構成図である。

【００８５】図７は、個人認証部２による個人認証の第１の具体例による個人認証手順を示すフローチャートである。

【００８６】図６に示すように、個人認証部２は、ＩＣカードリーダ３１に挿入されたＩＣカード３２と通信することによって利用者の認証を行う。

【００８７】図７に示すフローチャートに基づいてその認証手順を説明する。

【００８８】はじめに、個人認証部２からＩＣカードリーダ（読取部）３１を介してＩＣカード３２に対し、第１認証コード生成要求を送信する（ステップＳ１）。
【００８９】ＩＣカード３２は、ＩＣカードリーダ３１を介して第１認証コード生成要求を受信して第１認証コードを生成し、それをＩＣカードリーダ３１を介して個人認証部２へ送信する（ステップＳ２）。
【００９０】個人認証部２では、第１認証コードを受信すると、ＩＣカード３２内に格納されている内部認証キーを用いて所定の演算を行うことにより、第１応答コードを生成し、それをＩＣカードリーダ３１を介してＩＣカード３２へ送信する（ステップＳ３）。
【００９１】ＩＣカード３２は、ＩＣカードリーダ３１を介して第１応答コードを受信すると、第１認証コードコードに対して外部認証キーを用いて所定の演算を行うことにより、第１応答コードとその計算結果とを比較する（ステップＳ４）。
【００９２】続いて、ＩＣカード３２からＩＣカードリーダ３１を介して個人認証部２に対して、第２認証コード生成要求を送信する（ステップＳ５）。
【００９３】個人認証部２は、第２認証コードをを生成して、ＩＣカードリーダ３１を介してＩＣカード３２へ送信する（ステップＳ６）。
【００９４】ＩＣカード３２では、ＩＣカードリーダ３１を介して第２認証コードを受信すると、ＩＣカード３２内に格納されている内部認証キーを用いて、所定の演算を行うことにより、第２応答コードを生成して、それをＩＣカードリーダ３１を介して個人認証部２へ送信する（ステップＳ６）。
【００９５】個人認証部２は第２応答コードを受信すると、この第２認証コードに外部認証キーを用いて所定の演算を行うことにより、第２応答コードとその計算結果とを比較する（ステップＳ６）。
【００９６】個人認証部２は、このような手順で計算結果を比較することにより、個人認証を行う。
【００９７】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記個人認証部２は、認証情報が書き込まれたＩＣカード３２と、前記ＩＣカードに書き込まれた認証情報を読み取るＩＣカード読取部３１とを備え、前記個人認証部２とＩＣカード読取部３１との間の通信に暗号化通信を用いることを特徴とするデジタルデータ記録再生システムが提供される。
【００９８】（第２の具体例）図８は、個人認証部２による個人認証の第２の具体例を示す要部の構成図である。
【００９９】図８に示すように、この第２の具体例によると、個人認証部２は、生体情報入力装置３５と通信することによって利用者の認証を行う。
【０１００】生体情報入力装置３５は、光カード３３に書き込まれている生体情報３６を読み取るための光カードリーダ３１Ａと生の生体情報を入力するための生体情報入力部３４とにより構成される。
【０１０１】光カード３３には、カード作成時にあらかじめ本人であることを保証する生体情報を、例えば、生の生体情報から照合に適した特徴量という形態に変換し、それをさらに暗号化して保存しておくものとする。
【０１０２】ここでは、生体情報として指紋を例にとって、個人認証について説明する。
【０１０３】はじめに、個人認証部２が、出力部３７に対して入力要請のメッセージ、例えば、「指を生体情報入力部へ置いて、ボタンを押して下さい」を表示する。
【０１０４】利用者がそのメッセージを見て指を生体情報入力部３４に置き、ボタン３４Ａを押すと、生体情報入力部３４での指紋のスキャンが始まり、この生体情報入力部３４でスキャンされたデータが、個人認証部２へ送信される。
【０１０５】この生体情報入力部３４でのスキャンが完了すると、光カードリーダ部３１Ａに挿入された光カード３３にあらかじめ本人であることを保証する生体情報として書き込まれている生体情報３６が個人認証部２に送信される。
【０１０６】個人認証部２では、生体情報入力部３４でスキャンされた生体情報を特徴量に変換するとともに、続いて光カード３３から送られてきた生体情報３６の復号化を行う。
【０１０７】そして、個人認証部２では、生体情報入力部３４でスキャンされた生体情報を特徴量に変換したものと、光カード３３から送られてきた生体情報３６を照合することによって利用者が正当な利用者であるか否かの判定を行うことにより、利用者が正当な利用者である場合にのみ、当該システムの使用を許可する。
【０１０８】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記個人認証部は、生体情報を入力するための生体情報入力部を備え、前記生体情報入力部により入力された生体情報に基づいて個人認証を行うことを特徴とするデジタルデータ記録再生システムが提供される。
【０１０９】（改竄検出部３による改竄検出の具体例）次に、以上のような図１の実施形態における改竄検出部３による改竄検出の具体例について説明する。
【０１１０】（第１の具体例）図９は、改竄検出部３による改竄検出の第１の具体例を示す要部の構成図である。
【０１１１】図１０は、改竄検出部３による改竄検出の第１の具体例による改竄検出手順を示すフローチャートである。
【０１１２】図９に示すように、改竄検出部３は、Ｉ／Ｏ制御手段７を介して、保存装置１２に挿入された保存媒体１３に保存されている各データ２４の照合を行う照

合部３ａを有している。

【０１１３】そして、この改竄検出部３の照合部３ａは、利用者が保存媒体１３に保存されている各データ２４に対して修正や削除を行ったときに、それを検出するために機能するものである。

【０１１４】ここでは、利用者が保存媒体１３に保存されているデータ１に対して修正を行った場合についての改竄検出手順を図１０に示すフローチャートに基づいて説明する。

【０１１５】はじめに、改竄検出部３（の照合部３ａ）は、Ｉ／Ｏ制御手段７を通じて保存装置１２に挿入されている保存媒体１３のデータ２４を読み出す（ステップＳ２７）。

【０１１６】続いて、改竄検出部３（の照合部３ａ）は、この読み出されたデータ２４に対する電子署名を算出する（ステップＳ２８）。

【０１１７】ここで、電子署名はデータ２４の内容から一意に計算される識別子で、算出の方法はあらかじめ決めておくものとする。

【０１１８】改竄検出部３（の照合部３ａ）は、電子署名の算出が終了すると、Ｉ／Ｏ制御手段７を介して、保存媒体１３にデータ２４が書き込まれたときに、それと共に書き込まれている電子署名２５を読み出す（ステップＳ２９）。

【０１１９】続いて、改竄検出部３（の照合部３ａ）は、計算された電子署名と保存媒体１３より読み出された電子署名２５との照合を行う（ステップＳ３０）。

【０１２０】この場合、改竄検出部３（の照合部３ａ）は、計算された電子署名と保存媒体１３より読み出された電子署名２５との両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。

【０１２１】そして、改竄検出部３（の照合部３ａ）は、前記両者の照合結果として、両者が一致していた場合には、保存媒体１３に保存されていたデータが改竄されていないことが保証され、両者が不一致の場合には、データが改竄されていることを検出する。

【０１２２】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部３は、前記計算機本体１５に接続された保存部１２の各データファイル（保存媒体１３）に対して記録されている電子署名２５と、前記保存部１２の各データファイル（保存媒体１３）から所定の算出式に基づいて計算される照合用電子署名と、を照合する照合部３ａとを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【０１２３】（第２の具体例）この第２の具体例において、改竄検出部３による改竄検出のを示す要部の構成は図９と同じである。

【０１２４】この第２の具体例において、改竄検出部３による改竄検出の手順は、図１０に示すフローチャートと同じである。

【０１２５】図９に示すように、改竄検出部３は、Ｉ／Ｏ制御手段７を介して、保存部１２に挿入された保存媒体１３に保存されているすべてのデータ２４の照合を行う照合部３ａを有している。

【０１２６】そして、この第２の具体例においては、利用者が保存媒体１３を保存部１２に挿入したときに、改竄検出部３（の照合部３ａ）が機能するものである。

【０１２７】ここでは、利用者が保存媒体１３に保存されているデータ１に対して修正を行った場合についての改竄検出手順を図１０に示すフローチャートに基づいて説明する。

【０１２８】はじめに、改竄検出部３（の照合部３ａ）は、Ｉ／Ｏ制御手段７を通じて保存部１２に挿入されている保存媒体１３のすべてのデータ２４を読み出す（ステップＳ２７）。

【０１２９】続いて、改竄検出部３（の照合部３ａ）は、この読み出されたデータ２４に対する電子署名を算出する（ステップＳ２８）。

【０１３０】ここで、電子署名はデータ２４の内容から一意に計算される識別子で、算出の方法はあらかじめ決めておくものとする。

【０１３１】改竄検出部３（の照合部３ａ）は、電子署名の算出が終了すると、Ｉ／Ｏ制御手段７を介して、保存媒体１３にデータ２４が書き込まれたときに、それと共に書き込まれている電子署名２５を読み出す（ステップＳ２９）。

【０１３２】続いて、改竄検出部（の照合部３ａ）３は、計算された電子署名と保存媒体１３より読み出された電子署名２５との照合を行う（ステップＳ３０）。

【０１３３】この場合、改竄検出部（の照合部３ａ）３は、計算された電子署名と保存媒体１３より読み出された電子署名２５との両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。

【０１３４】そして、改竄検出部（の照合部３ａ）３は、照合結果として、前記両者が一致していた場合には、保存媒体１３に保存されていたデータが改竄されていないことが保証され、両者が不一致の場合には、データが改竄されていることを検出する。

【０１３５】なお、図９中の属性データ３８は、後述する属性管理部６や履歴データ保存部５によって管理されるものである。

【０１３６】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部３は、前記計算機本体１５に接続された保存部１２の各データファイルに対して記録されている電子署名と、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用電子署名と、を照合するための照合部３ａとを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【０１３７】（履歴データ保存部５の具体例）次に、以上のような図１の実施形態における履歴データ保存部５の具体例について説明する。

【０１３８】図１１は、履歴データ保存部５の具体例を示す要部の構成図である。

【０１３９】図１１に示すように、履歴データ保存部５は、利用者が保存装置１２に挿入されている保存媒体１３に保存されている各データ２４に対して修正や削除を行ったときに、属性データ３８に履歴を追加する。

【０１４０】この履歴データ保存部５が管理する属性データ３８は、図１１では保存装置（保存部）１２内に書き込むようにしているが、大容量の外部記憶装置がある場合には、その外部記憶装置に書き込むようにしても良い。

【０１４１】また、履歴データの内容は、利用者を識別するための使用者名を含むユーザーＩＤ、利用の日時を示すアクセス日時、利用者がどのような作業を行ったかを示すアクセス種別、使用した保存装置（保存部）１２を特定するための保存装置識別子を含む保存装置のＩＤなどがある。

【０１４２】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記履歴データ記録部（保存部）５は、履歴データとして利用者を識別するための使用者名と、利用の日時を示す利用日時と、利用者がどのような作業を行ったかを示すアクセス種別と、使用した保存装置を特定するための保存装置識別子と、を前記データ保存部へ記録することを特徴とする記載のデジタルデータ記録再生システムが提供される。

【０１４３】（アクセスログ記録部４の具体例）次に、以上のような図１の実施形態におけるアクセスログ記録部４の具体例について説明する。

【０１４４】図１２は、アクセスログ記録部４の具体例を示す要部の構成図である。

【０１４５】図１２に示すように、アクセスログ記録部４は、利用者が個人認証部２でシステムの使用が許可された場合、あるいはシステムの使用を終了したときにアクセスログを書き込む。

【０１４６】外部記憶装置１２のアクセスログに対して、利用開始あるいは利用終了日時を含むアクセス日時、利用者を識別するための利用者名に対応したユーザ名、利用開始あるいは利用終了の種別を示すＬｏｇ－ｉｎ／Ｌｏｇ－ｏｕｔ、などのアクセス結果を書き込む。

【０１４７】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記アクセスログ記録部４は、利用開始あるいは利用終了日時と、利用者を識別するための利用者名と、利用開始あるいは利用終了の種別と、を前記データ保存部に記録することを特徴とするデジタルデータ記録再生システムが提供される。

【０１４８】（属性管理部６の具体例）次に、以上のような図１の実施形態における属性管理部６の具体例について説明する。

【０１４９】図１３は、属性管理部６の具体例を示す要部の構成図である。

【０１５０】図１３に示すように、属性管理部６は、利用者がデータのステータスの変更を行ったときに、属性データ３８の更新を行う。

【０１５１】この属性データ３８の内容は、ファイル名、データの内容がファイルであるのかディレクトリであるのか識別するためのファイルタイプ、ファイルのサイズ、ファイルへのアクセス制限を示すファイルアトリビュート、ファイルが原本ファイル、仮原本ファイル、謄本ファイル、一般ファイルの区別をするためのファイルステータス、ファイルの作成者、ファイルの作成日時、ファイルの更新者、ファイルの更新日時、保存期間などがあり、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを含む。

【０１５２】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記属性管理部６は、少なくとも属性データとして、データがオリジナルであることを示すオリジナル識別子と、データがバックアップであることを示すバックアップ識別子とを管理することを特徴とするデジタルデータ記録再生システムが提供される。

【０１５３】（Ｉ／Ｏ制御部７の具体例）次に、以上のような図１の実施形態におけるＩ／Ｏ制御部７の具体例について説明する。

【０１５４】（第１の具体例）図１４は、Ｉ／Ｏ制御部７の第１の具体例を示す要部の構成図である。

【０１５５】図１４に示すように、Ｉ／Ｏ制御部７は、保存装置（保存部）１２に挿入された保存媒体１３のデータの入出力手順を規定する。

【０１５６】例えば、利用者が保存媒体１３へアクセスしようとするとき、はじめに、Ｉ／Ｏ制御部７内の媒体種別判定部３９は、保存装置（保存部）１２に挿入されている保存媒体１３が専用保存媒体かあるいは一般保存媒体であるか判断する。

【０１５７】そして、保存媒体１３が専用保存媒体である場合には、Ｉ／Ｏ制御部７内の第１暗号化／復号化部４０を介してデータの入出力を行う。

【０１５８】まず、利用者が保存媒体１３へデータの書き込みを行うと、第１暗号化／復号化部４０は、暗号化部として働き、ここを通過するデータを所定の手続きにより暗号化する。

【０１５９】また、利用者が保存媒体１３からデータの読み出しを行うと、第１暗号化／復号化部４０は、復号化部として働き、ここを通過するデータを所定の手続き

により復号化する。

【０１６０】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記制御部８は、さらに、前記データ保存部１２内の保存媒体１３上のデータにアクセスするためのＩ／Ｏ制御部７を備え、このＩ／Ｏ制御部７は、前記保存媒体を識別するための保存媒体識別部３９と、データの情報を暗号化するための暗号化部４０と、暗号化されたデータを復号するための復号化部４０とを備えることを特徴とするデジタルデータ記録再生システムが提供される。

【０１６１】（第２の具体例）図１５は、Ｉ／Ｏ制御部７の第２の具体例を示す要部の構成図である。

【０１６２】図１５に示すように、Ｉ／Ｏ制御部７は、保存装置１２に挿入された保存媒体１３のデータの入出力手順を規定する。

【０１６３】例えば、利用者が保存媒体１３へアクセスしようとするとき、はじめに、Ｉ／Ｏ制御部７内の媒体種別判定部３９は、保存装置１２に挿入されている保存媒体１３が専用保存媒体かあるいは一般保存媒体であるか判断する。

【０１６４】そして、保存媒体１３が専用保存媒体である場合には、階層的に構成されたＩ／Ｏ制御部７内の第１暗号化／復号化部４０から第ｎ暗号化／復号化部４１を介してデータの入出力を行う。

【０１６５】まず、利用者が保存媒体１３へデータの書き込みを行うと、第１暗号化／復号化部４０は、第１暗号化部として働き、ここを通過するデータを所定の手続きにより暗号化すると共に、そのデータを第２暗号化／復号化部へと送る。

【０１６６】第２暗号化／復号化部も、第１暗号化／復号化部４０と同様に、暗号化部として働き、そこを通過するデータを所定の手続きにより暗号化するというように、以下、ｎ階層の暗号化／復号化部を介してデータの書き込みを行う。

【０１６７】また、利用者が保存媒体１３からデータの読み出しを行うと、第１暗号化／復号化部４０は、第１復号化部として働き、ここを通過するデータを所定の手続きにより復号化すると共に、そのデータを第２暗号化／復号化部へと送る。

【０１６８】第２暗号化／復号化部も、第１暗号化／復号化部４０と同様に、復号化部として働き、そこを通過するデータを所定の手続きにより復号化するというように、以下、ｎ階層の暗号化／復号化部を介してデータの復号化を行う。

【０１６９】このように、Ｉ／Ｏ制御部７の第２の具体例では、暗号化を階層的に行うことにより、データの機密性を高くすることができる。

【０１７０】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記暗号化部４０と復号化部４０は、それぞれ階層的な構造により暗号化レベルを変化することができることを特徴とするデジタルデータ記録再生システムが提供される。

【０１７１】（システム起動の具体例）次に、以上のような図１の実施形態におけるシステム起動の具体例について説明する。

【０１７２】図１６は、システム起動の具体例を示す要部のフローチャートである。

【０１７３】図１６に示すように、利用者により実行処理開始が入力部１４より指示される（ステップＳ４２）と、制御部８内の復号化部は、所定の暗号化方式により暗号化された各部を復号し、実行可能状態にする（ステップＳ４３）。

【０１７４】続いて、実行可否判定部１によって、各部の実行環境が正当であるか否かが判断され（ステップＳ４４）、正当である場合には制御部８が起動されて起動状態になるが、正当でない場合には、起動されない。

【０１７５】（システム終了の具体例）次に、以上のような図１の実施形態におけるシステム終了の具体例について説明する。

【０１７６】図１７は、システム終了の具体例を示す要部のフローチャートである。

【０１７７】図１７に示すように、すべての処理が終了し、利用者により終了処理開始４６が実行される（ステップＳ４６）と、制御部８内の終了部が実行され、制御部８が終了する（ステップＳ４７）。

【０１７８】制御部８が終了すると同時に、制御部８内の暗号化部が実行され、制御部８が暗号化されることにより（ステップＳ４８）、実行不可能状態になって終了する（ステップＳ４９）。

【０１７９】（新規データ登録処理の具体例）次に、以上のような図１の実施形態における新規データ登録処理の具体例について説明する。

【０１８０】図１８は、新規データ登録処理についての具体例を示す要部のフローチャートである。

【０１８１】図１８に示すように、新規登録処理開始が実行される（ステップＳ５０）と、正当な利用者であるか確認するため、個人認証部２で利用者の認証確認が行われる（ステップＳ５１）。

【０１８２】図１８では毎回、認証を行うように記しているが一度、認証を行えば２回目以降は認証を行う必要はない。

【０１８３】続いて、利用者の情報を記録するため、アクセスログ記録部４での処理が実行される（ステップＳ５２）。

【０１８４】続いて、新規に登録するデータの属性の情報を記録するため属性管理部６での処理が実行される（ステップＳ５３）。

【０１８５】続いて、データの履歴情報を記録するため履歴データ記録部５での処理が実行される（ステップＳ５４）。

【０１８６】続いて、データの保存媒体１３への書き込みが行われ（ステップＳ５５）、書き込みが行われたデータに対する電子署名を作成する処理が実行され（ステップＳ５６）た後、新規登録処理を終了する（ステップＳ５７）。

【０１８７】図１８では、属性管理部６での処理、履歴データ記録部５での処理、保存媒体１３への書き込み、電子署名作成の順番で処理を行うように記してあるが、これらの実行順序は問わない。

【０１８８】（登録データの更新の具体例）次に、以上のような図１の実施形態における登録データの更新の具体例について説明する。

【０１８９】図１９は、登録データの更新の具体例を示す要部のフローチャートである。

【０１９０】図１９に示すように、登録データ更新処理開始が実行される（ステップＳ５８）と、正当な利用者であるか確認するため、個人認証部２で利用者の認証確認が行われる（ステップＳ５９）。

【０１９１】図１９では毎回、認証を行うように記しているが一度、認証を行えば２回目以降は認証を行う必要はない。

【０１９２】続いて、利用者の情報を記録するため、アクセスログ記録部４での処理が実行される（ステップＳ６０）。

【０１９３】続いて、更新されるデータが不正利用者によって書き換え、変更されていないことを確認するため改竄検出部３での処理が実行される（ステップＳ６１）。

【０１９４】改竄検出部３によりデータの書き換え、変更がなされていることが確認されると、改竄通知が実行され（ステップＳ６２）、利用者にデータの書き換え、変更がなされていることを通知して更新を行うことなく処理を終了する（ステップＳ６３）。

【０１９５】改竄検出部３において、データの書き換え、変更が行われていないことが確認された場合には、更新するデータの属性の情報を記録するため属性管理部６での処理が実行される（ステップＳ６４）。

【０１９６】続いて、データの履歴情報を記録するため履歴データ記録部５での処理が実行される（ステップＳ６５）。

【０１９７】続いて、データの保存媒体１３への書き込みが行われ（ステップＳ６６）、書き込みが行われたデータに対する電子署名を作成する処理が実行され（ステップＳ６７）た後、登録データ更新処理を終了する（ステップＳ６８）。

【０１９８】図１９では、属性管理部６での処理、履歴データ記録部５での処理、保存媒体１３への書き込み、電子署名作成の順番で処理を行うように記してあるが、これらの実行順序は問わない。

【０１９９】（登録データの削除の具体例）次に、以上のような図１の実施形態における登録データの削除の具体例について説明する。

【０２００】図２０は、登録データの削除の具体例を示す要部のフローチャートである。

【０２０１】図２０に示すように、登録データ削除処理開始が実行される（ステップＳ６９）と、正当な利用者であるか確認するため、個人認証部２で利用者の認証確認が行われる（ステップＳ７０）。

【０２０２】図２０では毎回、認証を行うように記しているが一度、認証を行えば２回目以降は認証を行う必要はない。

【０２０３】続いて、利用者の情報を記録するため、アクセスログ記録部４での処理が実行される（ステップＳ７１）。

【０２０４】続いて、更新されるデータが不正利用者によって書き換え、変更されていないことを確認するため改竄検出部３での処理が実行される（ステップＳ７２）。

【０２０５】改竄検出部３によりデータの書き換え、変更がなされていることが確認されると、改竄通知が実行され（ステップＳ７３）、利用者にデータの書き換え、変更がなされていることを通知して削除を行うことなく処理を終了する（ステップＳ７４）。

【０２０６】改竄検出部３において、データの書き換え、変更が行われていないことが確認された場合には、保存媒体１３に登録されているデータのうち削除するデータの削除が行われる（ステップＳ７５）。

【０２０７】続いて、その削除データの属性の情報を記録したデータ、電子署名が削除が行われる。（ステップＳ７６）。

【０２０８】（登録データの複製の具体例）次に、以上のような図１の実施形態における登録データの複製の具体例について説明する。

【０２０９】図２１は、登録データの複製の具体例を示す要部のフローチャートである。

【０２１０】図２１に示すように、登録データ複製処理開始が実行される（ステップＳ７７）と、正当な利用者であるか確認するため、個人認証部２で利用者の認証確認が行われる（ステップＳ７８）。

【０２１１】図２１では毎回、認証を行うように記しているが一度、認証を行えば２回目以降は認証を行う必要はない。

【０２１２】続いて、利用者の情報を記録するため、アクセスログ記録部４での処理が実行される（ステップＳ７９）。

【０２１３】続いて、更新されるデータが不正利用者によって書き換え、変更されていないことを確認するため改竄検出部３での処理が実行される（ステップＳ８０）。

【０２１４】改竄検出部３によりデータの書き換え、変

更がなされていることが確認されると、改竄通知が実行され（ステップＳ８１）、利用者にデータの書き換え、変更がなされていることを通知して複製を行うことなく処理を終了する（ステップＳ８２）。

【０２１５】改竄検出部３においてデータの書き換え、変更が行われていないことが確認された場合には、データの属性確認を行うため属性確認部６での処理が実行される（ステップＳ８３）。

【０２１６】データを複製するには、複製（作成）元データが原本である必要があるため、データの属性の確認を行うものであって、作成元データが原本でない場合には複製の作成を行うことができないので、複製を行うことなく処理を終了する（ステップＳ８２）。

【０２１７】しかるに、複製（作成）元データが原本である場合には、複製（作成）元データの属性の情報を記録するために、属性管理部６での処理が実行される（ステップＳ８４）。

【０２１８】続いて、データの履歴情報を記録するため履歴データ記録部５での処理が実行される（ステップＳ８５）。

【０２１９】続いて、データの保存媒体１３への書き込みが行われ（ステップＳ８６）、書き込みが行われたデータに対する電子署名を作成処理が実行され（ステップＳ８７）た後、複製（作成）先データの属性の情報を記録するために、属性管理部６での処理が実行される（ステップＳ８８）。

【０２２０】続いて、データの履歴情報を記録するために、履歴データ記録部５での処理が実行される（ステップＳ８９）た後、登録データ複製処理を終了する（ステップＳ９０）。

【０２２１】

【発明の効果】従って、以上説明したように、本発明によれば、ネットワーク設備のない所でも容易に運用することができる低コストのデータ保存装置として実現することが可能なデジタルデータ記録再生システムを提供することができる。

【図面の簡単な説明】

【図１】図１は、本発明の一実施の形態として適用されるデジタルデータ記録再生システムの構成を示すブロック図である。

【図２】図２は、図１の実行可否判定部１による実行可否判定の第１の具体例を示す要部の構成図である。

【図３】図３は、図１の実行可否判定部１による実行可否判定の第２の具体例を示す要部の構成図である。

【図４】図４は、図１の実行可否判定部１による実行可否判定の第３の具体例を示す要部の構成図である。

【図５】図５は、図１の実行可否判定部１による実行可否判定の第４の具体例を示す要部の構成図である。

【図６】図６は、図１の個人認証部２による個人認証の第１の具体例を示す要部の構成図である。

【図７】図７は、図１の個人認証部２による個人認証の第１の具体例による個人認証手順を示すフローチャートである。

【図８】図８は、図１の個人認証部２による個人認証の第２の具体例を示す要部の構成図である。

【図９】図９は、図１の改竄検出部３による改竄検出の第１の具体例を示す要部の構成図である。

【図１０】図１０は、図１の改竄検出部３による改竄検出の第１の具体例による改竄検出手順を示すフローチャートである。

【図１１】図１１は、図１の履歴データ保存部５の具体例を示す要部の構成図である。

【図１２】図１２は、図１におけるアクセスログ記録部４の具体例を示す要部の構成図である。

【図１３】図１３は、図１の属性管理部６の具体例を示す要部の構成図である。

【図１４】図１４は、図１におけるＩ／Ｏ制御部７の第１の具体例を示す要部の構成図である。

【図１５】図１５は、図１におけるＩ／Ｏ制御部７の第２の具体例を示す要部の構成図である。

【図１６】図１６は、図１におけるシステム起動の具体例を示す要部のフローチャートである。

【図１７】図１７は、図１におけるシステム終了の具体例を示す要部のフローチャートである。

【図１８】図１８は、図１のシステムにおける新規データ登録処理についての具体例を示す要部のフローチャートである。

【図１９】図１９は、図１のシステムにおける登録データの更新の具体例を示す要部のフローチャートである。

【図２０】図２０は、図１のシステムにおける登録データの削除の具体例を示す要部のフローチャートである。

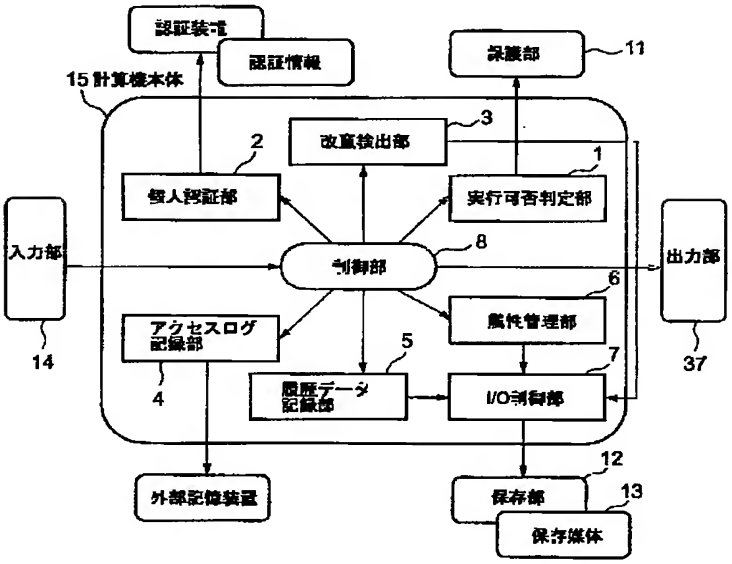
【図２１】図２１は、図１のシステムにおける登録データの複製の具体例を示す要部のフローチャートである。

【符号の説明】

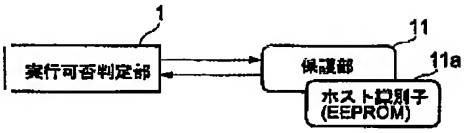
１４…データ入力部、
１５…計算機本体、
３７…データ出力部、
７…Ｉ／Ｏ制御部、
１２…データ保存部、
１３…保存媒体、
２…個人認証部、
４…アクセスログ記録部、
３…改竄検出部、
５…履歴データ記録部、
６…属性管理部、
８…制御部、
１…実行可否判定部、
１１…保護部、
１１ａ，１１ｂ…読み出し専用不揮発性メモリ、
１６…ホスト識別子、

１７…中央演算装置、
１８～２０…ｎ個のホスト識別子読み取り部ａ～ｎ、
２１～２３データ列、
２４…データ、
２５…電子署名、
３１…ＩＣカードリーダ、
３２…ＩＣカード、
３５…生体情報入力装置、
３４…生体情報入力部、
３４Ａ…ボタン、
３３…光カード、
３１Ａ…光カードリーダ部、
３６…生体情報、
３ａ…照合部、
３８…属性データ、
３９…媒体種別判定部、
４０…第１暗号化／復号化部、
４１…第ｎ暗号化／復号化部。

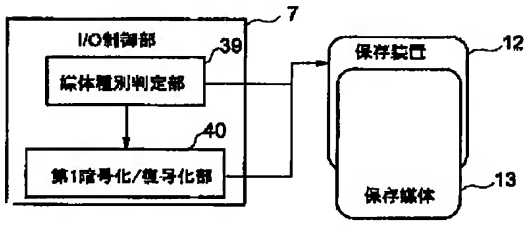
【図１】



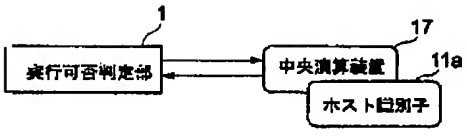
【図２】



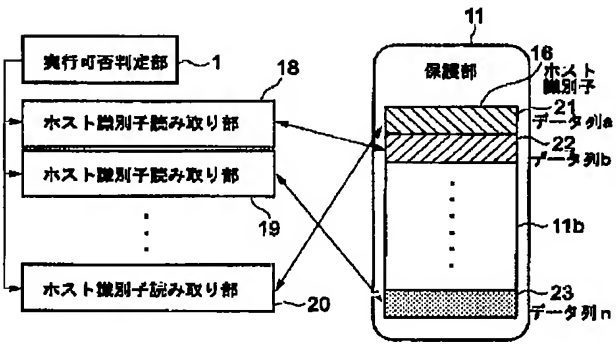
【図１４】



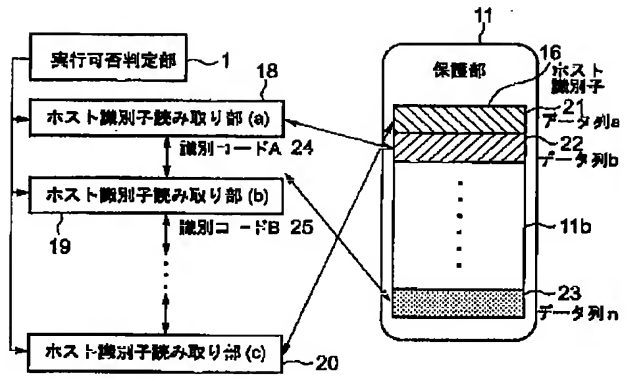
【図３】



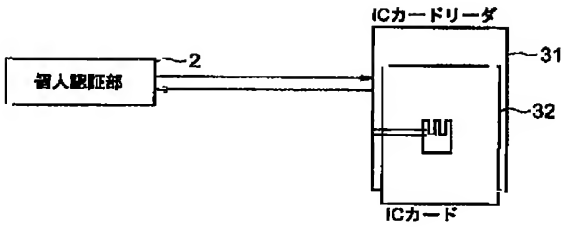
【図４】



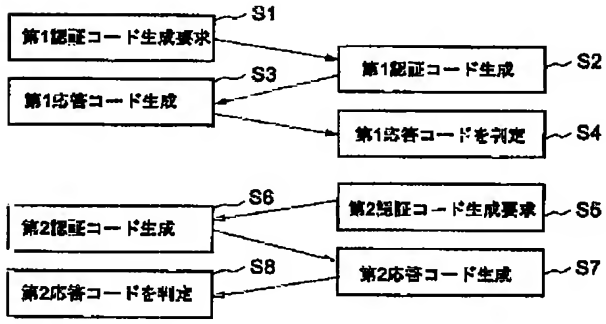
【図５】



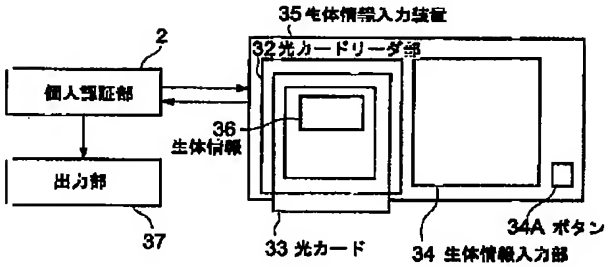
【図６】



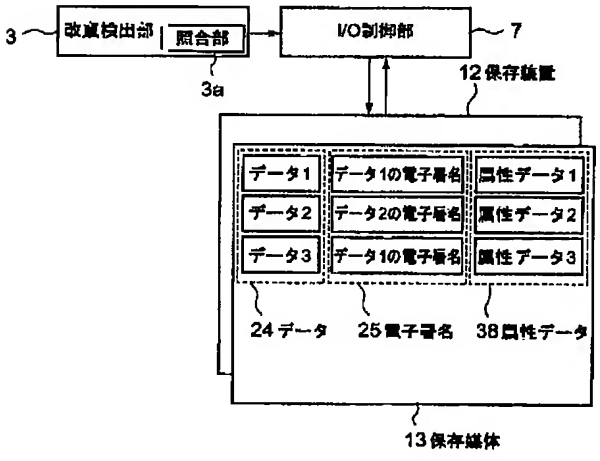
【図７】



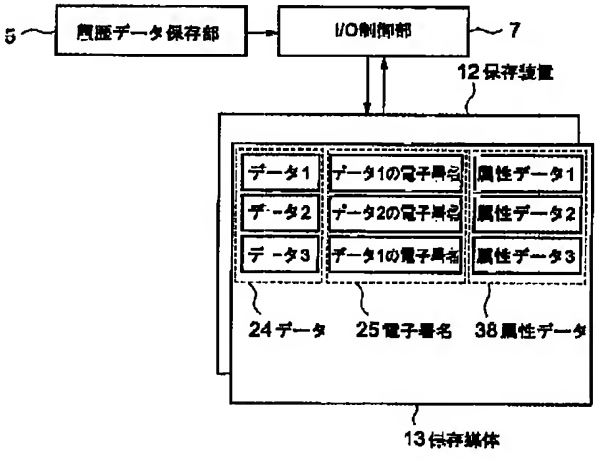
【図８】



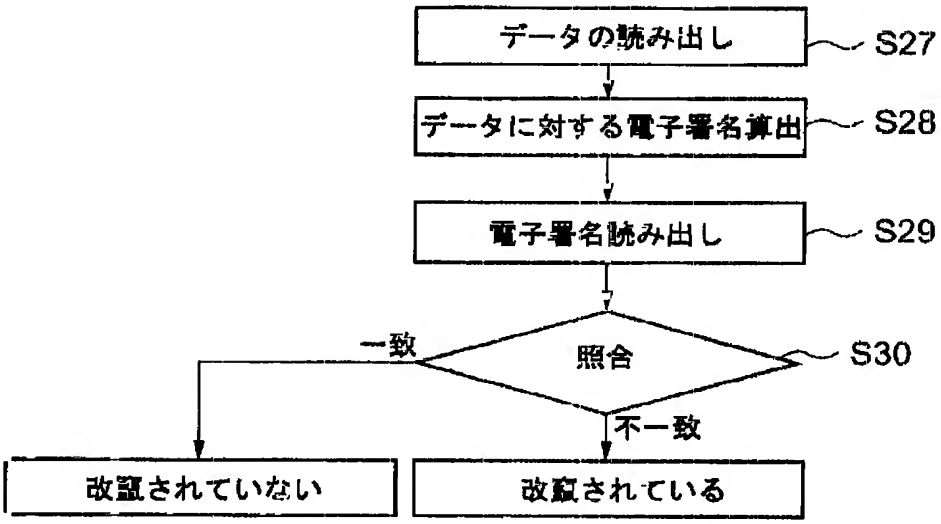
【図９】



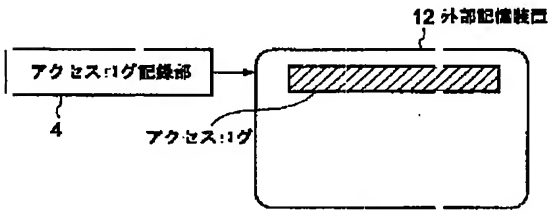
【図１１】



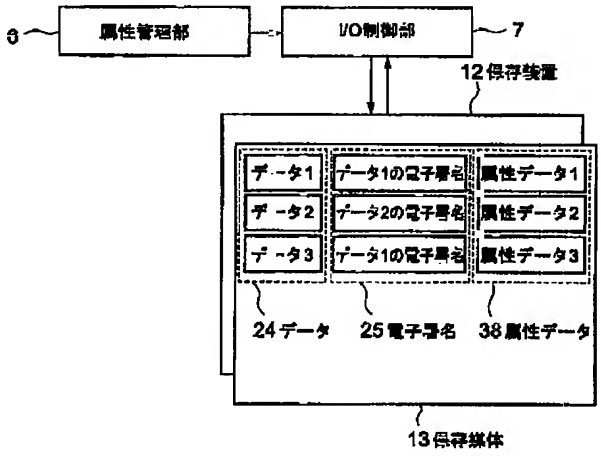
【図１０】



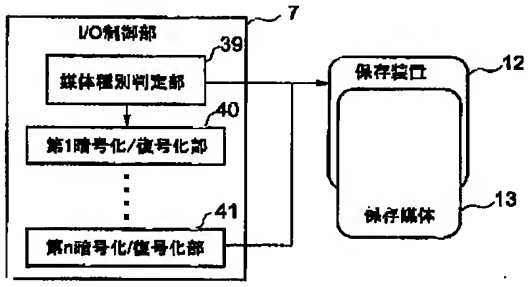
【図１２】



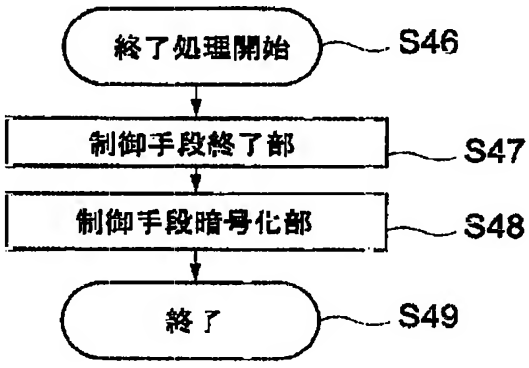
【図１３】



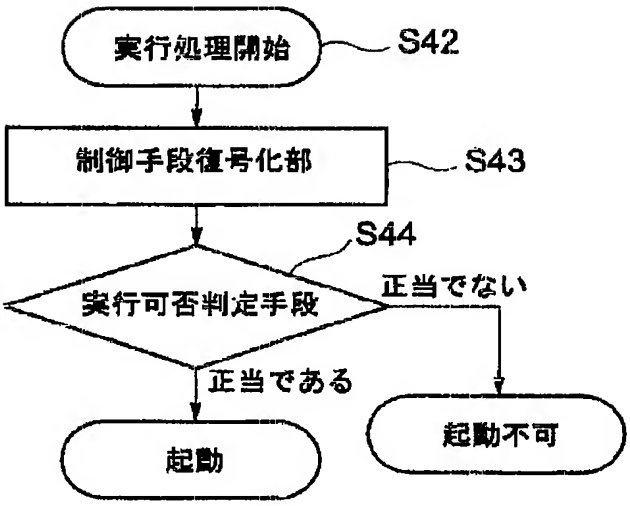
【図１５】



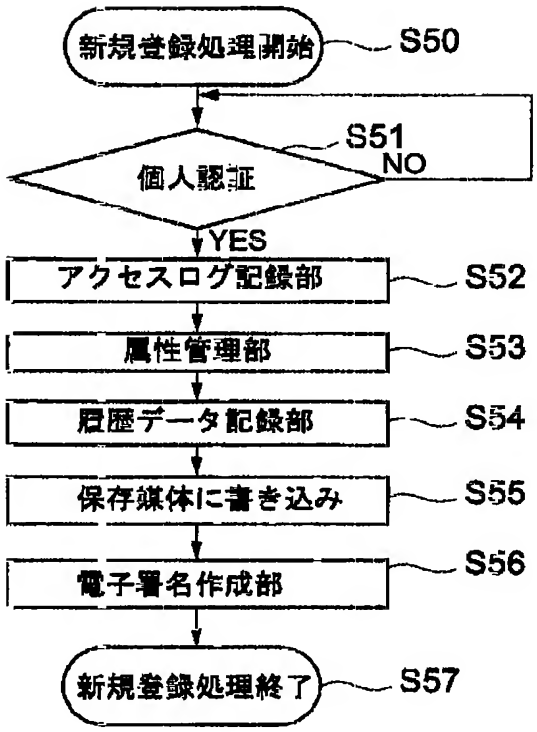
【図１７】



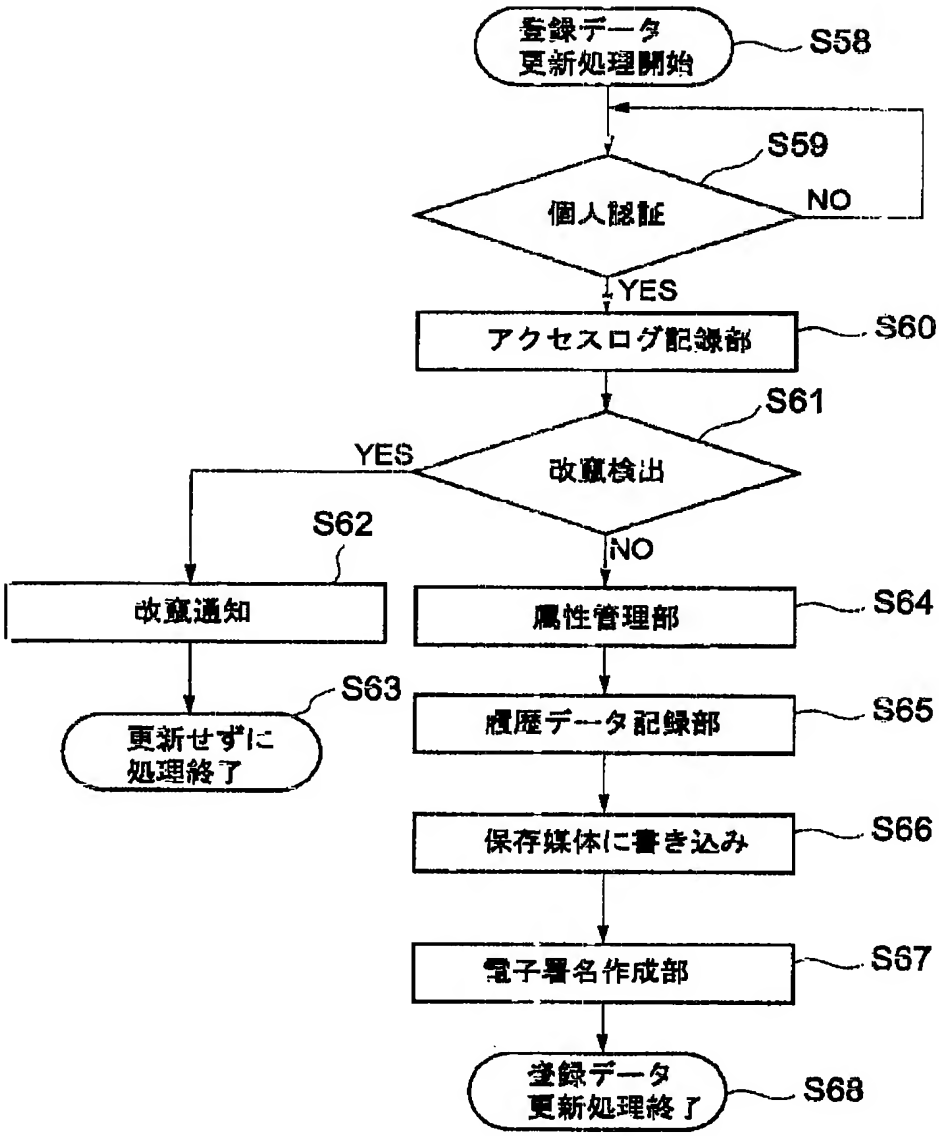
【図16】


実行処理開始
S42
制御手段復号化部
S43
S44
実行可否判定手段
正当でない
正当である
起動
起動不可

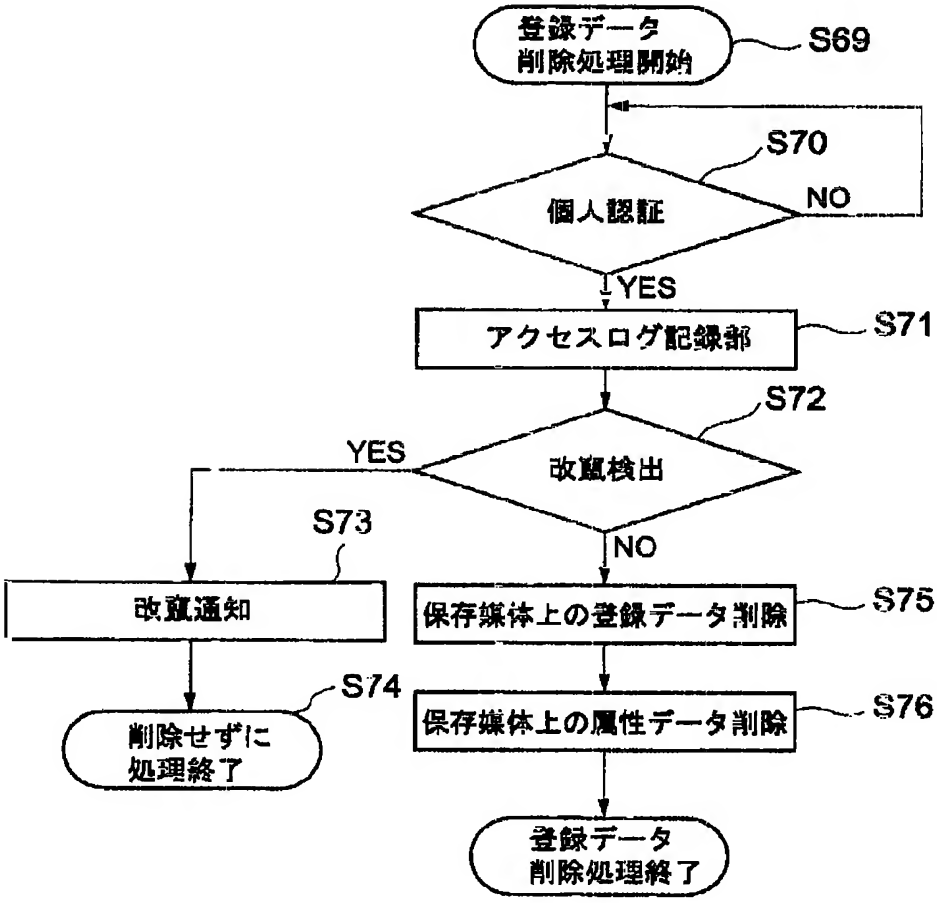
【図18】


新規登録処理開始
S50
S51
個人認証
NO
YES
アクセスログ記録部
S52
属性管理部
S53
履歴データ記録部
S54
保存媒体に書き込み
S55
電子署名作成部
S56
新規登録処理終了
S57

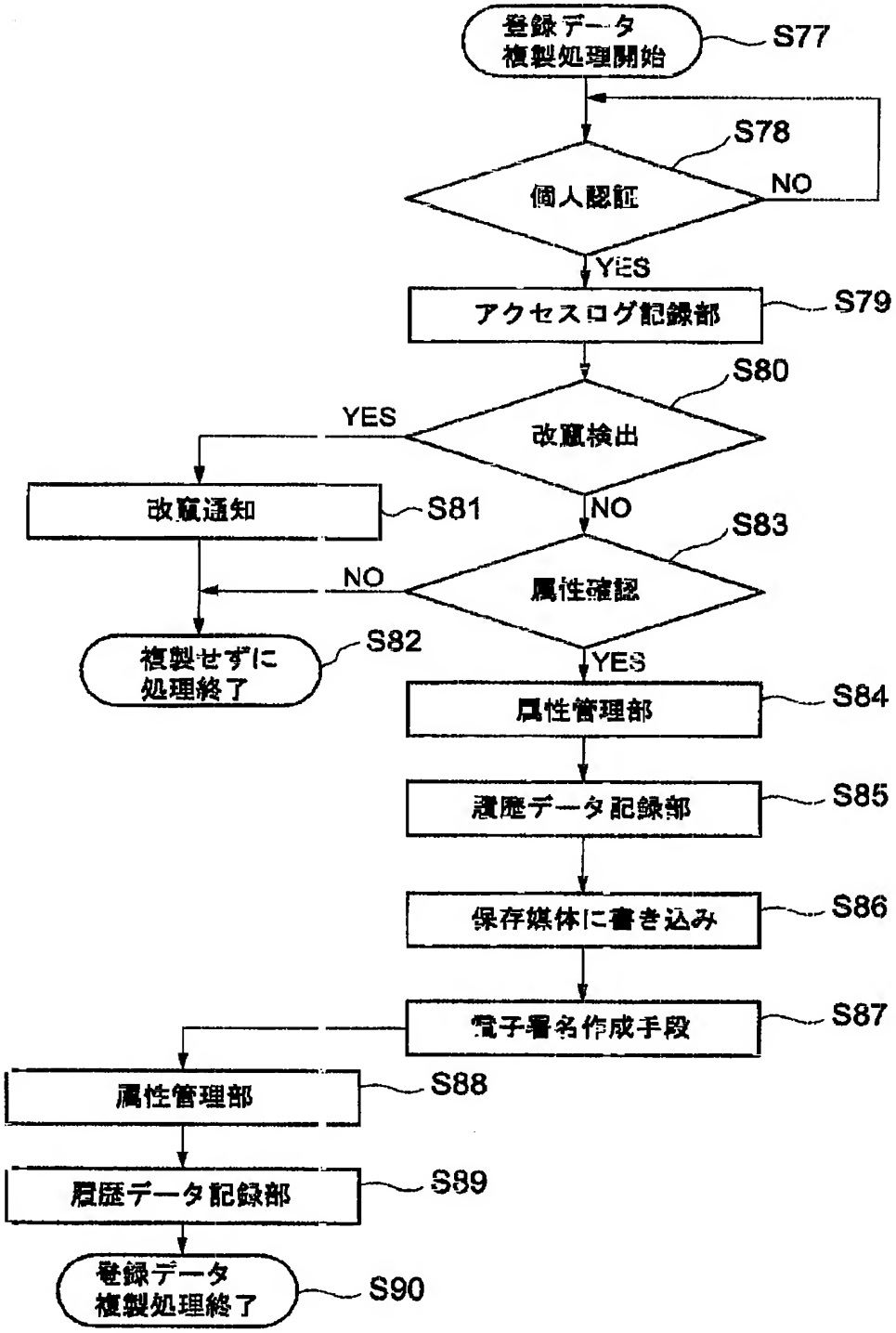
【図19】


登録データ
更新処理開始
S58
S59
個人認証
NO
YES
アクセスログ記録部
S60
S61
改竄検出
YES
NO
S62
改竄通知
S63
更新せずに
処理終了
属性管理部
S64
履歴データ記録部
S65
保存媒体に書き込み
S66
電子署名作成部
S67
登録データ
更新処理終了
S68

【図20】


登録データ
削除処理開始
S69
S70
個人認証
NO
YES
アクセスログ記録部
S71
S72
改竄検出
YES
NO
S73
改竄通知
保存媒体上の登録データ削除
S75
S74
削除せずに
処理終了
保存媒体上の属性データ削除
S76
登録データ
削除処理終了

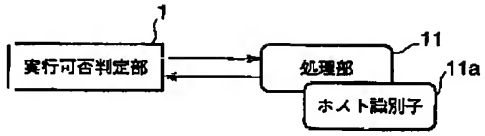
【図21】


登録データ
複製処理開始
S77
S78
個人認証
NO
YES
アクセスログ記録部
S79
S80
改竄検出
YES
NO
改竄通知
S81
S83
属性確認
NO
YES
複製せずに
処理終了
S82
属性管理部
S84
履歴データ記録部
S85
保存媒体に書き込み
S86
電子署名作成手段
S87
属性管理部
S88
履歴データ記録部
S89
登録データ
複製処理終了
S90

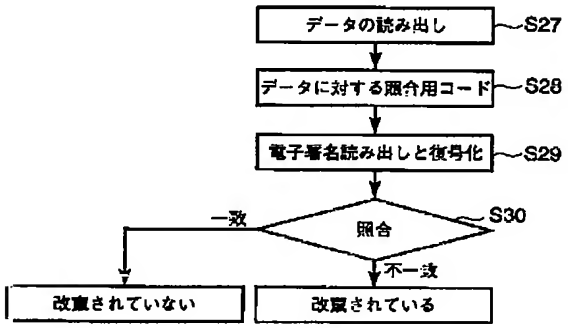
【手続補正書】
【提出日】平成１２年7月１８日（２０００．７．１８）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項３
【補正方法】変更
【補正内容】
【請求項３】前記計算機本体に備えられた処理部にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行うことを特徴とする請求項１記載のデジタルデータ記録再生システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項８
【補正方法】変更
【補正内容】
【請求項８】前記改竄検出部は、
前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、
前記保存部の各データファイルから所定の算出式に基づいて計算される照合用コードと、
を照合する照合部とを備えることを特徴とする請求項１記載のデジタルデータ記録再生システム。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】請求項９
【補正方法】変更
【補正内容】
【請求項９】前記改竄検出部は、
前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、
前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用コードと、
を照合するための照合部とを備えることを特徴とする請求項１記載のデジタルデータ記録再生システム。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００４
【補正方法】変更
【補正内容】
【０００４】このような問題を解決するため、近時、公表されている「原本性保証電子保存システムの開発」（創造的ソフトウエア育成事業及びエレクトリック・コマース推進事業に係る最終成果発表会１９９８）においては、２台の電子計算機をそれぞれ保存装置とホスト装置というように位置づけ、それらをＬＡＮなどのネットワークで接続して使用している。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正内容】
【００１３】また、本発明によると、上記課題を解決するために、（３）　前記実行可否判定部は、前記計算機本体に備えられた処理部にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子を読み出して判定を行うことを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正内容】
【００１８】また、本発明によると、上記課題を解決するために、前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、前記保存部の各データファイルから所定の算出式に基づいて計算される照合用コードと、を照合する照合部とを備えることを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正内容】
【００１９】また、本発明によると、上記課題を解決するために、前記改竄検出部は、前記計算機本体に接続された保存部の各データファイルに対して記録されている電子署名を復号化して得られる照合用コードと、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用コードと、を照合するための照合部とを備えることを特徴とする（１）記載のデジタルデータ記録再生システムが提供される。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００４９
【補正方法】変更
【補正内容】
【００４９】図３に示すように、実行可否判定部１は、前記計算機本体１５に備えられている処理部１７にあらかじめ格納されているホスト識別子１６を取得することにより、前記制御部８による各部に対する動作制御命令を実行する環境が正当な環境であるか否かを判断する。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００５１
【補正方法】変更
【補正内容】
【００５１】はじめに、実行可否判定部１は、前記計算機本体１５に備えられている処理部１７に対してホスト識別子取得要求を送信する。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００５２
【補正方法】変更
【補正内容】
【００５２】そして、処理部１７では、実行可否判定部１からのホスト識別子取得要求を受信すると、実行可否判定部１に対してホスト識別子１６を送信する。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００５４
【補正方法】変更
【補正内容】
【００５４】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記実行可否判定部は、前記計算機本体１１に備えられた処理部１７にあらかじめ書き込まれている前記動作制御命令が実行される環境が正当な環境であることを保証するためのホスト識別子１６を読み出して判定を行なうことを特徴とするデジタルデータ記録再生システムが提供される。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】０１１９
【補正方法】変更
【補正内容】
【０１１９】続いて、改竄検出部３（の照合部３ａ）は、計算された照合用コードと保存媒体１３より読み出された電子署名２５を復号化して得られる照合用コードとの照合を行う（ステップＳ３０）。
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】０１２０
【補正方法】変更
【補正内容】
【０１２０】この場合、改竄検出部３（の照合部３ａ）は、計算された照合用コードと保存媒体１３より読み出された電子署名２５を復号化して得られる照合用コードとの両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】０１２２
【補正方法】変更
【補正内容】
【０１２２】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部３は、前記計算機本体１５に接続された保存部１２の各データファイル（保存媒体１３）に対して記録されている電子署名２５を復号化して得られる照合用コードと、　前記保存部１２の各データファイル（保存媒体１３）から所定の算出式に基づいて計算される照合用コードと、を照合する照合部３ａとを備えることを特徴とするデジタルデータ記録再生システムが提供される。
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】０１２９
【補正方法】変更
【補正内容】
【０１２９】続いて、改竄検出部３（の照合部３ａ）は、この読み出されたデータ２４に対する照合用コードを算出する（ステップＳ２８）。
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】０１３０
【補正方法】変更
【補正内容】
【０１３０】ここで、照合用コードはデータ２４の内容から一意に計算される識別子で、算出の方法はあらかじめ決めておくものとする。
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】０１３１
【補正方法】変更
【補正内容】
【０１３１】そして、改竄検出部３（の照合部３ａ）は、照合用コードの算出が終了すると、Ｉ／Ｏ制御手段７を介して、保存媒体１３にデータ２４が書き込まれたときに、それと共に書き込まれている電子署名２５を読み出して復号化する（ステップＳ２９）。
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】０１３２
【補正方法】変更
【補正内容】
【０１３２】続いて、改竄検出部（の照合部３ａ）３は、計算された照合用コードと保存媒体１３より読み出された電子署名２５を復号化した照合用コードとの照合を行う（ステップＳ３０）。
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】０１３３

【補正方法】変更
【補正内容】
【０１３３】この場合、改竄検出部（の照合部３ａ）３は、計算された照合用コードと保存媒体１３より読み出された電子署名２５を復号化した照合用コードとの両者を単位データ毎に比較し、すべてのデータの比較が終了したら照合が完了する。
【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】０１３６
【補正方法】変更
【補正内容】
【０１３６】すなわち、以上のような具体例によると、前記デジタルデータ記録再生システムにおいて、前記改竄検出部３は、前記計算機本体１５に接続された保存部１２の各データファイルに対して記録されている電子署名を復号化した照合用コードと、前記保存部に保存されているすべてのデータファイルに基づいて作成された照合用コードとを照合するための照合部３ａとを備えることを特徴とするデジタルデータ記録再生システムが提供される。
【手続補正２１】
【補正対象書類名】図面
【補正対象項目名】図３
【補正方法】変更
【補正内容】
【図３】



【手続補正２２】
【補正対象書類名】図面
【補正対象項目名】図１０
【補正方法】変更
【補正内容】
【図１０】



フロントページの続き

Ｆターム(参考)　5C064 CC01 CC06
5D044 BC06 CC04 DE48 DE49 GK17
5J104 AA07 AA09 KA01 KA04 KA16
LA06 NA35 NA38
9A001 BB02 BB03 BB04 BB05 CC02
DD09 EE03 HH21 HH23 JJ08
JJ12 KK37 KK60 KZ16 LL03